(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08272742 A

(43) Date of publication of application: 18.10.96

(51) Int. Cl G06F 15/00
G09C 1/00
H04L 9/32

(21) Application number: 07072781

(22) Date of filing: 30.03.95

(71) Applicant: HITACHI LTD

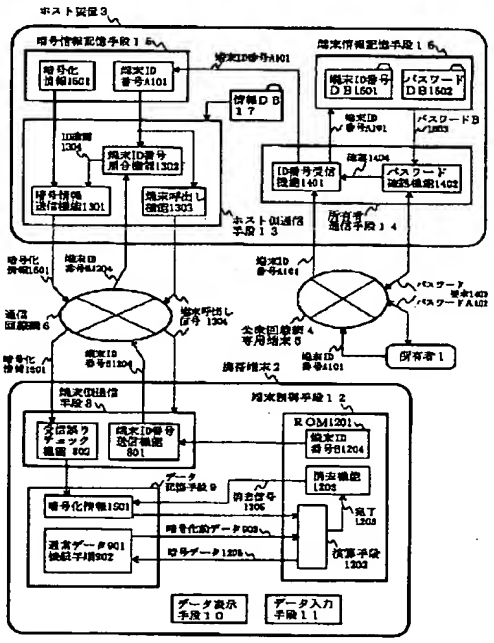
(72) Inventor: YOKOZAWA TATSU
SHIMIZU HIROSHI

(54) DATA LEAK PREVENTION SYSTEM

(57) Abstract:

PURPOSE: To prevent data from leaking when a portable terminal is lost or stolen by ciphering internal stored data with ciphering information sent from a host device and deleting the ciphering information at the end of the ciphering.

CONSTITUTION: When the owner 1 becomes aware that the portable terminal 2 is lost and performs data leak preventing operation through public telephone line 4, an owner communication means 14 of the host device 3 receives the terminal ID number, a terminal information storage means 16 takes the password out on the basis of the terminal ID number, and a password confirming function 1402 confirms whether the password that the owner has inputted matches with the taken-out password. When their coincidence is confirmed, a cipher information transmitting function 1301 sends the cipher information, stored in a cipher information storage means 15, to the terminal 2. A terminal control means 12 of the terminal 2 ciphers normal data and a connection procedure stored in a data storage means 9 according to the ciphering information and after the ciphering ends, an erasing function 1203 generates an erasure signal to erases the ciphering information stored in the data storage means 9.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－272742

(43)公開日　平成８年(1996)10月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　15/00	３３０	9364－5L	Ｇ０６Ｆ　15/00	３３０Ｃ	
Ｇ０９Ｃ　1/00		7259－5Ｊ	Ｇ０９Ｃ　1/00		
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	Ａ	

審査請求　未請求　請求項の数９　ＯＬ　（全 19 頁）

(21)出願番号　特願平7－72781

(22)出願日　平成７年(1995)３月30日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　横沢　達
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所映像メディア研究所内

(72)発明者　清水　宏
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所映像メディア研究所内

(74)代理人　弁理士　小川　勝男

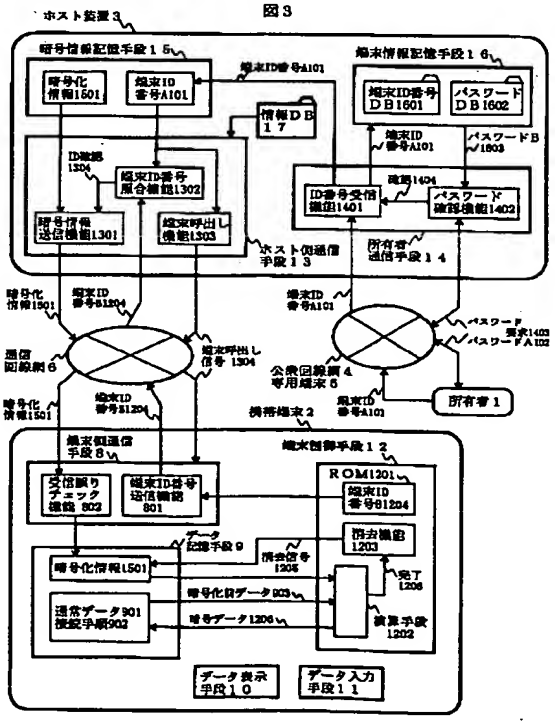
(54)【発明の名称】　データ漏洩防止システム

(57)【要約】

【構成】データを暗号化する演算手段１２０２と、データを記憶するデータ記憶手段９と公衆回線や一般加入回線を介して所有者と通信を行う所有者通信手段１４と、その所有者が入力する端末ＩＤ番号と端末側での暗号化に使用する暗号化情報を記憶する暗号情報記憶手段１５と、暗号化情報を携帯端末へ送信するホスト側通信手段１３とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段９と、ホスト装置と通信をする機能を持つ端末側通信手段８と、暗号化情報を消去する機能１２０３と、暗号化処理をするための演算手段を有する携帯端末を設ける。

【効果】携帯端末の所有者は端末の紛失や盗難に伴うデータ漏洩を最小限にとどめることが可能になる。

図３



【特許請求の範囲】

【請求項１】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力する為のデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段により入力される情報と、暗号化に必要な暗号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、

前記携帯端末がデータ記憶手段に通常のデータ以外にホスト装置から送信された暗号化情報と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に前記暗号化情報を消去する機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ＩＤ番号を記憶する機能、前記演算手段に前記暗号化情報により前記データ記憶手段に記憶されたデータを暗号化する機能、端末側通信手段にホスト装置との通信を開始するときに端末ＩＤ番号を送信する機能と、暗号化情報を受信して受信誤りをチェックし、データ記憶手段へ入力する機能を備え、前記ホスト装置が端末情報記憶手段に各端末につけられた端末ＩＤ番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して所有者が入力する端末ＩＤ番号を受信する機能と、端末情報記憶手段から端末ＩＤ番号を元にパスワードを取り出し、本人からの通信であることを前記パスワードにより確認する機能と、前記確認された端末ＩＤ番号を前記暗号情報記憶手段に登録する機能、ホスト側通信手段に前記暗号情報記憶手段に記憶された端末ＩＤ番号と、端末から通信回線網を介して送信された端末ＩＤ番号を照合し、登録された携帯端末との通信であることを検出する機能と、端末ＩＤ番号により前記番号の端末を呼出す機能と、前記暗号情報記憶手段から取り出した暗号化情報を携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ＩＤ番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、通信回線網を介して携帯端末が前記接続手順を用いるか、またはホスト装置が前記端末の端末ＩＤ番号を用いて通信が開始され、携帯端末からホスト装置へ端末ＩＤ番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から暗号化情報がホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化情報は受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記暗号化情報を用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化情報を消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無い場合でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項２】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力するためのデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段より入力される情報と、復号化に必要な復号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデータ以外にホスト装置から送信された復号化情報を記憶する機能、前記読み出し専用記憶手段に前記携帯端末である事を示す為の端末ＩＤ番号を記憶する機能、前記演算手段に前記復号化情報により前記データ記憶手段に記憶された暗号化済みデータを復号化する機能、端末側通信手段にホスト装置からの呼出しに対して前記端末ＩＤ番号を受信応答として送信する機能と、復号化情報を受信して受信誤りをチェックし、データ記憶手段へ入力する機能を備え、また、前記ホスト装置が端末情報記憶手段に各端末につけられた端

末ＩＤ番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して所有者が入力する端末ＩＤ番号を受信する機能と、端末情報記憶手段から端末ＩＤ番号を元にパスワードを取り出し、本人からの依頼であることを前記パスワードにより確認する機能と、前記確認された端末ＩＤ番号をホスト側通信手段に入力する機能、ホスト側通信手段に公衆回線網を介して入力された端末ＩＤ番号で携帯端末を呼出す機能と、前記携帯端末が受信応答として送信した端末ＩＤ番号により接続を確認する機能と、前記暗号情報記憶手段の復号化情報を読み出して前記携帯端末へ送信する機能を備えることで、既に前記携帯端末のデータ記憶手段のデータが暗号化された状態で、所有者が前記データを復号化するために、所有者が最寄りの電話機または専用端末により前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力した前記パスワードが確認されると、前記端末ＩＤ番号は復号化を指定された端末としてホスト側通信手段へ入力され、通信回線網を介して端末の呼出しが行われ、ホスト側通信手段が端末側から端末ＩＤ番号で応答を受けて通信が確立されると、ホスト側通信手段により暗号情報記憶手段の復号化情報が通信回線網を介して端末へ送信され、一方、端末側通信手段が受信した復号化情報は前記データ記憶手段に記憶され、演算手段が前記復号化情報を用いてデータ記憶手段のデータを復号化することで、復号化の為の情報をデータ記憶手段に記憶していない携帯端末でも、通信回線網を介して前記データ記憶手段に記憶された暗号データを参照可能なデータに変換できる事を特徴とするデータ漏洩防止システム。

【請求項３】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力するためのデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段により入力される情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデータ以外に暗号化と復号化の為の暗号化情報を記憶する機能と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に前記暗号化情報を端末側通信手段を介して外部より受信するコマンドにより消去できる機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ＩＤ番号を記憶する機能、前記演算手段に日常動作においてデータ記憶手段の内の暗号化情報以外のデータを常に暗号化する機能と、必要なときのみ暗号化済みのデータを復号化する機能、端末側通信手段にホスト装置との通信を開始するときに端末ＩＤ番号を送信する機能と、ホスト装置から通信回線網を介して送信される暗号化情報の消去コマンドを受信する機能を備え、また、前記ホスト装置が端末情報記憶手段に各端末につけられた端末ＩＤ番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して前記端末ＩＤ番号が入力されると、端末情報記憶手段から端末ＩＤ番号を元にパスワードを取り出し、本人からの通信であることを前記パスワードにより確認する機能と、前記確認された端末ＩＤ番号を暗号情報記憶手段に登録する機能、ホスト側通信手段に通信回線網を介して端末ＩＤ番号で端末を呼出す機能と、前記暗号情報記憶手段に記憶された端末ＩＤ番号と端末から送信された端末ＩＤ番号を照合し、登録された携帯端末との通信であることを検出する機能と、前記検出により前記暗号情報記憶手段から取り出した前記暗号化情報を消去するコマンドを、携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末のデータ復号化機能を無効にするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ＩＤ番号が復号化機能を無効にする端末として暗号情報記憶手段に記憶され、この後、携帯端末が前記接続手順を用いるか、またはホスト装置が前記端末の端末ＩＤ番号を用いて通信を開始して、携帯端末からホスト装置へ端末ＩＤ番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、前記暗号化情報を消去するコマンドが前記携帯端末へ送信され、前記消去コマンドを受信した携帯端末が、端末制御手段により前記データ記憶手段内の暗号化情報を消去して復号化機能を無効にすることで、携帯端末が手元に無い場合でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項４】請求項１において、前記暗号化情報を暗号化プログラムと暗号キーとし、前記携帯端末の演算手段

に前記暗号化プログラムを実行し、前記暗号キーに基づいて前記データ記憶手段に記憶された前記暗号化情報を除くデータを暗号化する機能、前記端末制御手段に暗号化プログラムと暗号キーを消去する機能、端末側通信手段に前記暗号キーと暗号化プログラムを暗号情報として受信して前記データ記憶手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として暗号化プログラムと暗号キーを予め記憶する機能、ホスト側通信手段に暗号情報記憶手段から取り出した暗号化プログラムと暗号キーを携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータを暗号化するために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ＩＤ番号が暗号化する端末として暗号情報記憶手段に登録され、この後、携帯端末が前記接続手順を用いて、またはホスト装置が前記端末の端末ＩＤ番号を用いて通信が開始され、携帯端末からホスト装置へ端末ＩＤ番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から暗号化プログラムと暗号キーがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化プログラムと暗号キーは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記暗号化プログラムと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化プログラムと暗号キーを消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無く、さらに暗号化の為のプログラムも内蔵していない携帯端末でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項５】請求項１において、前記暗号化情報を暗号キーと制御コマンドとし、前記携帯端末が前記読み出し専用記憶手段に予めプログラムを記憶し、前記演算手段に前記制御コマンドに従って前記プログラムを実行し、前記暗号キーにより前記データ記憶手段に記憶されたデータを暗号化する機能、前記端末制御手段に暗号キーを消去する機能、端末側通信手段に前記暗号キーと制御コマンドを暗号情報として受信し、前記暗号キーは前記データ記憶手段へ、前記制御コマンドは前記端末制御手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として制御コマンドと暗号キーを予め記憶する機能、ホスト側通信手段に前記暗号情報記憶手段から取り出した制御コマンドと暗号キーを携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ＩＤ番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、携帯端末が前記接続手順を用いて、またはホスト装置が前記端末の端末ＩＤ番号を用いて通信が開始され、携帯端末からホスト装置へ端末ＩＤ番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から制御コマンドと暗号キーがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記制御コマンドと暗号キーは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記制御コマンドと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号キーを消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無くても、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項６】請求項１において、前記暗号化情報を暗号化プログラムとし、前記携帯端末が前記読み出し専用記憶手段に予め暗号キーを記憶し、前記演算手段に前記暗号化プログラムに従って前記プログラムを実行し、前記暗号キーにより前記データ記憶手段に記憶されたデータを暗号化する機能、前記端末制御手段に暗号化プログラムを消去する機能、端末側通信手段に前記暗号化プログラムを暗号情報として受信し、前記データ記憶手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として暗号化プログラムを予め記憶する機能、ホスト側通信手段に前記暗号情報記憶手段から取り出した暗号化プログラムを携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ＩＤ番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ＩＤ番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、携帯端末が通信回線網を介して前記接続手順を用いるか、またはホスト装置が前記端末の端末ＩＤ番号を用いて通信が開始され、携帯端末からホスト装置へ端末ＩＤ番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確

認され、前記端末である場合には、暗号情報記憶手段から暗号化プログラムがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化プログラムは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記プログラムと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化プログラムを消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無く、さらに暗号化の為のプログラムも内蔵していない携帯端末でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項７】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力するためのデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、復号化に必要な復号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデータと所有者がデータ入力手段から入力する暗号化情報と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に後述する暗号化要求を受けると、暗号化で使用する暗号化情報の入力を前記データ表示手段を介して所有者に要求する機能と、前記暗号化情報の入力により暗号化開始指示を端末側通信手段に入力する機能と、前記暗号化情報を消去する機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ＩＤ番号を記憶する機能、前記演算手段に前記暗号化情報により前記データ記憶手段のデータを暗号化する機能と、前記暗号化を後述する送信終了により開始する機能、データ入力手段に所有者が暗号化要求を前記端末制御手段に入力する機能と、前記暗号化情報を前記データ記憶手段に入力する機能、端末側通信手段に暗号化開始指示を受けると前記接続手順でホスト装置と接続する為に端末ＩＤ番号を送信する機能と、前記暗号化情報を復号化情報として前記ホスト装置へ送信する機能と、前記復号化情報をホスト装置へ送信した事を前記演算手段に送信終了により通知する機能を備え、また、前記ホスト装置が端末情報記憶手段に予め登録された各端末の端末ＩＤ番号を記憶する機能、ホスト側通信手段に前記端末情報記憶手段に記憶された端末ＩＤ番号と端末から送信された端末ＩＤ番号を照合し、登録された携帯端末との通信であることを検出する機能と、前記照合された端末ＩＤ番号を前記暗号情報記憶手段に登録する機能と、受信した前記復号化情報を前記照合された端末ＩＤ番号と共に前記暗号情報記憶手段に記憶する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、暗号化要求指示を前記データ入力手段より入力すると、前記データ表示手段を介して前記端末制御手段から暗号化情報の入力を要求され、所有者が前記要求に従って前記データ入力手段から暗号化情報を入力すると、前記暗号化情報が前記データ記憶手段に記憶され、これにより端末制御手段から暗号化開始指示が前記端末側通信手段に入力され、前記通信手段が前記接続手順により通信回線網を介して前記ホスト装置を呼出し、接続すると端末ＩＤ番号と復号化情報が送信され、一方、呼出しを受けたホスト装置ではホスト側通信手段により端末ＩＤ番号が照合され、検出された前記端末ＩＤ番号は続いて受信される復号化情報暗号と共に暗号情報記憶手段に記憶され、次いで、前記端末側通信手段が送信終了を前記演算手段に入力すると、前記演算手段が前記暗号化情報を用いて前記データ記憶手段にあるデータの暗号化を開始し、暗号化が完了すると前記端末制御手段により前記暗号化情報が消去され、暗号を解くための情報が端末内から無くなることで、手元の携帯端末に記憶されたホスト装置への接続手順を含むデータを暗号化して参照不能にすると共に、これを復号化する為の復号化情報をホスト装置に保存することにより、安全にデータ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項８】請求項１，３，４，５または６において、前記携帯端末の端末制御手段に前記ホスト装置から暗号化情報または制御コマンドが送信されたことを検出する機能と、前記検出を受けると前記データ記憶手段に記憶されたデータの漏洩防止処理をしている間、データ表示手段により後述するメッセージを表示する機能、前記読み出し専用記憶手段にホスト装置との接続処理を実行中であることを示すメッセージを記憶する機能を備えることで、第三者が携帯端末を取得して、ホスト装置を不正に利用する目的で接続操作を行い、接続処理が完了したとき、前記端末制御手段によりホスト装置から暗号化情報または制御コマンドが送信されたことが検出され、前記読み出し専用記憶手段から取り出したメッセージがデータ表示手段により第三者に提示され、表示されている間に漏洩防止処理が行われることで、実際には接続が完了していても、第三者に暗号化処理が実行されていることを認識させないことを特徴としたデータ漏洩防止シス

テム。

【請求項９】請求項１，３，４，５または６において、前記ホスト装置のホスト側通信手段が端末ＩＤ番号の照合機能に加えて、前記情報記憶手段から情報を取出す前に、前記携帯端末に対して特定の暗証番号の入力を求める機能と、前記入力された暗証番号が誤った事を計数し、予め設定された回数以上になると暗号化情報を携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により携帯端末を紛失し、前記携帯端末が第三者により取得されて、ホスト装置の前記情報記憶手段から情報が取出されるとき、第三者が特定の回数以上暗証番号の入力を間違えると自動的に前記携帯端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、携帯端末内部またはこの端末に接続されるデータ通信システムに記憶されたデータの漏洩防止システムに関する。

【０００２】

【従来の技術】記憶装置内のデータが第三者へ漏洩することを防止する手段として、従来より何らかの操作をする前（例えばデータファイルへの接続）に利用者へ暗唱番号の入力を要求する方法や、データ自身の暗号化が用いられている。特に、携帯する事を前提とする端末には、オフィスで据置にして利用される端末には無い紛失や盗難といった危険性を持っているため、端末内のデータを守るため必ず上記の様なデータの保護手段が備わっている。

【０００３】このようなシステムの例としては特開平１－１２６７９３号公報のようにＩＣカードに記憶されたデータを守るために、同じ暗号キーを端末とＩＣカードが持ち、相互に暗号化したデータを復号化して認証し合うことで同ＩＣカードが正規端末で利用されている事を確認し、データの利用を許可するシステムや、特開平４－２３３６４７号公報のように利用者が入力する個人確認情報をＩＣカードにおいて確認し、正規利用者であることが確認されるとホストコンピュータを利用できるシステムなどがある。

【０００４】

【発明が解決しようとする課題】上記従来技術では、データの不正利用を防止する為に暗号キーや個人確認情報などを用いている。

【０００５】しかし、これら照合をする為のデータは、通常本体内またはＩＣカード内の記憶デバイスに所有者が操作できないように記憶された上、書き換えが可能でも不用意にデータが失われないようにするために、記憶保持には電源を必要としないことが多い。よって、もしも本体または本体とＩＣカードを共に紛失したり、盗難に遭うなどした場合、第三者が故意に内部の記憶デバイスを取り出し、同デバイス内のデータを読み取る装置を使用すれば、照合用データを入手することが可能で、これはすなわち端末内のデータの漏洩だけではなく、この端末で接続できるホスト装置内のデータも漏洩する可能性が有ることを示しており、安全性の観点から不十分である。

【０００６】また、紛失届けをホスト装置に出すことでホスト装置内のデータを守ることは出来るが、この場合、端末内のデータを守ることが出来ない。

【０００７】本発明の目的は、内部の記憶デバイスを取り出されるような場合でも、携帯端末内に記憶されたデータが漏洩するのを防止すること、紛失や盗難後でもデータ漏洩を防止出来るようにすること、またこの機能を必要に応じて所有者が簡単に解除できることにある。

【０００８】

【課題を解決するための手段】本発明は、上記目的を達成するために、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ＩＤ番号と、端末側での暗号化に使用する暗号化情報を記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、暗号化情報を携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、ホスト装置と通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号化情報を受信する機能を持つ端末側通信手段と、暗号化情報を消去する機能と、各携帯端末の端末ＩＤ番号を記憶する読み出し専用記憶手段と、暗号化処理をするための演算手段を持つ端末制御手段とを有する携帯端末を備える。

【０００９】また、本発明は、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、端末側での復号化に使用する復号化情報を記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、復号化情報を携帯端末へ送信する機能を持つホスト側通信手段を有するホスト装置と、ホスト装置からの呼出しに対して端末ＩＤ番号をホスト装置へ送信する機能と、復号化情報を受信する機能を持つ端末側通信手段と、各携帯端末の端末ＩＤ番号を記憶

する読み出し専用記憶手段と、復号化処理をするための演算手段と持つ端末制御手段と、所有者用のデータとホスト装置から送信された復号化情報を記憶する書換え可能なデータ記憶手段と、を有する携帯端末を備える。

【００１０】また、本発明は、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ＩＤ番号と暗号化情報を消す消去コマンドを記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、消去コマンドを暗号情報記憶手段から取り出し携帯端末へ送信する機能を持つホスト側通信手段を有するホスト装置と、所有者用のデータと暗号化と復号化の為の暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、各携帯端末毎の端末ＩＤ番号を記憶する読み出し専用記憶手段と、日常動作ではデータ記憶手段内のデータを常に暗号化し、必要なときのみ復号化する演算手段を持つ端末制御手段と、ホスト装置と通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号化情報の消去コマンドを受信する機能を持つ端末側通信手段と、消去コマンドを実行する端末制御手段とを有する携帯端末を備える。

【００１１】また発明は、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ＩＤ番号と、端末側での暗号化に使用する暗号化プログラムと暗号キーを記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、暗号化プログラムと暗号キーを携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化プログラムと暗号キーと、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、ホスト装置と通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号化プログラムと暗号キーを受信する機能を持つ端末側通信手段と、暗号化プログラムと暗号キーを消去する機能と、各携帯端末の端末ＩＤ番号を記憶する読み出し専用記憶手段と、暗号化プログラムにより暗号化処理をする演算手段を持つ端末制御手段とを有する携帯端末を備える。

【００１２】また、本発明は、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、暗号化処理を開始させる制御コマンドを発行するホスト制御装置と、照合された端末ＩＤ番号と、端末側での暗号化に使用する暗号キーを記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、暗号キーと制御コマンドを携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、ホスト装置と通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号キーと制御コマンドを受信する機能を持つ端末側通信手段と、所有者用のデータとホスト装置から送信された暗号キーと、ホスト装置との接続手順を記憶する書換え可能なデータ記憶手段と、暗号キーを消去する機能と、各携帯端末の端末ＩＤ番号を記憶する読み出し専用記憶手段と、ホスト装置から制御コマンドを受けて暗号化処理を開始する演算手段を持つ端末制御手段とを有する携帯端末を備える。

【００１３】また発明は、各端末の端末ＩＤ番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ＩＤ番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ＩＤ番号と、端末側での暗号化に使用する暗号化プログラムを記憶する暗号情報記憶手段と、照合された端末ＩＤ番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ＩＤ番号を照合する機能と、暗号化プログラムを携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化プログラムと、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、暗号化プログラムを消去する機能と、各携帯端末の端末ＩＤ番号と暗号キーを記憶する読み出し専用記憶手段と、暗号化プログラムにより暗号化処理をする演算手段を持つ端末制御手段と、ホスト装置と通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号化プログラムを受信する機能を持つ端末側通信手段とを有する携帯端末を備える。

【００１４】また発明は、各端末の端末ＩＤ番号を予め登録された端末情報記憶手段と、携帯端末から送信された端末ＩＤ番号を照合する機能と、端末から送信された復号化情報を受信するホスト側通信手段と、復号化情報と照合された端末ＩＤ番号を記憶する暗号情報記憶手段とを有するホスト装置と、所有者用のデータと暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、所有者が暗号化処理を要求すると暗号化情報の入力をデータ表示手段を介して所有者に促す機能と、暗号化情報を消去する機能と、各携帯端末の端末ＩＤ番号を記憶する読み出し専用記憶手段と、暗号情報がホスト装置に送信された後に暗号化処理をする演算手段を持つ端末制御手段と、データ記憶手段に記憶され

たデータを所有者に提示する為のデータ表示手段と、所有者が暗号化の要求と暗号化情報を入力する為のデータ入力手段と、ホスト装置と接続手順により通信を開始する時に端末ＩＤ番号をホスト装置へ送信する機能と、暗号化情報を復号化情報としてホスト装置へ送信する機能と、送信が終了したことを演算手段に通知する機能を持つ端末側通信手段とを有する携帯端末を備える。

【００１５】

【作用】本発明では、携帯端末がホスト装置から送信される暗号化情報により、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化情報を暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００１６】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【００１７】また本発明では、携帯端末がホスト装置から送信される復号化情報により、内部に記憶した暗号化済みデータの復号化を行うので、復号化の為の情報を内部に持たない携帯端末でも通信回線を介して所有者の指示により簡単に暗号化を解除できる。

【００１８】また本発明では、携帯端末が常に内部に記憶するデータの暗号化を行い、必要なときだけ暗号化に使用した情報を元に復号化を行うので、この暗号化情報を消去することにより、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００１９】また、通信回線を介してホスト装置から暗号化情報の消去を指示出来るので、端末が手元に無い状態でもデータが漏洩するのを防止できることになる。

【００２０】また本発明では、携帯端末がホスト装置から送信される暗号化プログラムと暗号キーにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化プログラムと暗号キーを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００２１】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【００２２】さらに、暗号化のためのプログラムを内蔵していない携帯端末でもデータの暗号化が可能となる。

【００２３】また本発明では、携帯端末がホスト装置から送信される暗号キーと制御コマンドにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号キーを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００２４】また、暗号キーと制御コマンドだけを通信回線を介してホスト装置から送信すればよいので、通信時間を短くでき、さらに通信回線を介して暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【００２５】また本発明では、携帯端末がホスト装置から送信される暗号化プログラムと、端末内部に固定値として記憶されている暗号キーにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化プログラムを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００２６】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【００２７】さらに、暗号化のためのプログラムのアルゴリズムを変更できるので、同じ暗号キーでも異なった暗号化が可能となる。

【００２８】また本発明では、所有者が携帯端末内のデータを暗号化する為に暗号情報を端末に入力すると、暗号化処理を開始する前に暗号情報をホスト装置の記憶手段に記憶させ、その後端末内にあるホスト装置への接続手順を含むデータの暗号化を行い、暗号化の終了で暗号化情報を削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【００２９】また、暗号化の指示を手元の携帯端末から任意の時点で行えるので、紛失や盗難の可能性が有る場合に対してデータ漏洩を予防することが出来る。

【００３０】

【実施例】以下、本発明を図示した各実施例によって説明する。

【００３１】＜第１実施例＞図１は、本発明の第一実施例の携帯端末間のデータ漏洩防止システムの概念図で、図２は本システムで携帯端末がホスト装置と接続されるまでの概略図で、図３は本実施例の詳細な図である。

【００３２】本実施例は、所有者が携帯端末を紛失、または盗難に遭った後を示したものである。

【００３３】図１で、２は携帯端末、１は携帯端末２の所有者、３は携帯端末２のホスト装置であり、後述するように携帯端末２に関する情報や所有者に提供する情報のデータベースを備える。４は所有者１とホスト装置３との間を接続する公衆回線網、５はホスト装置３に接続された専用端末、６は携帯端末２とホスト装置３との間を接続する通信回線網であり、有線または無線方式の公衆または専用回線網である。７は携帯端末２を不正に利用しようとしている不正利用者、１５０１は携帯端末２が暗号化をするための暗号化情報である。

【００３４】図２で、１７は所有者１が携帯端末２により取り寄せることが出来る各種情報が蓄積されたデータベースで情報ＤＢ、９０２は通信回線網６を介してホスト装置３と接続する為の呼出し方法を示した接続手順、３１は接続手順９０２により携帯端末２がホスト装置３と最初に接続されるゲート、１２０４は後述するＲＯＭ１２０１に記憶された携帯端末２に固有の端末ＩＤ番号Ｂ、３２は端末ＩＤ番号Ｂ１２０４を確認する第二のゲートで、ここで番号が確認されると携帯端末２がホスト装置３に接続される。また、９０４は所有者を認証するための所有者パスワードで、これが確認されると情報ＤＢ１７を操作できる。

【００３５】図３の携帯端末２では、１０１は所有者１が公衆回線網４または専用端末５でホスト装置３に入力する端末ＩＤ番号Ａ、１０２は同じく所有者１がホスト装置３へ入力するパスワードＡ８はホスト装置３からの呼出しを受信し、後述する端末ＩＤ番号送信機能８０１によって端末ＩＤ番号で応答する機能と、ホスト装置３と通信回線網６を介してデータ送受信をする為の端末側通信手段、９は書換えが可能でかつ一旦記憶操作が行われた後は外部からの給電無しに各種データを保持できるデータ記憶手段、１０はデータ記憶手段９に保持されたデータを所有者に提示するためのデータ表示手段、１１は所有者がデータを入力する為のデータ入力手段、１２は端末側通信手段８とデータ記憶手段９とデータ表示手段１０とデータ入力手段１１を制御する端末制御手段、１２０１は端末制御手段１２にありデータの書き込みが一度だけ出来る読み出し専用記憶手段（以下ＲＯＭ）、１２０２も端末制御手段１２にあり暗号化計算を行う演算手段、１２０６は演算機能１２０２が暗号化計算を終了すると出力する信号で完了、１２０３は完了１２０６を受けるとデータ記憶手段９に記憶された暗号化情報１５０１を消去する消去機能、１２０５は消去機能１２０３がデータ記憶手段９へ出力する消去信号、８０１は端末ＩＤ番号Ｂ８０１をホスト装置３へ送信する端末ＩＤ番号送信機能、８０２は通信回線網６を介して送信された暗号化情報１５０１を受信してその誤りをチェックした後、データ記憶手段９へ入力する受信誤りチェック機能、９０１はデータ記憶手段９に記憶された所有者１の使う通常データ、９０３は暗号化をする前のデータで暗号化前データ、１２０６は演算手段１２０２で暗号化された暗号データである。

【００３６】また、ホスト装置３では、１３は携帯端末２と通信回線網６を介してデータ送受信をする為のホスト側通信手段、１４は公衆回線網４または専用端末５を介して携帯端末２の所有者１と通信を行うための所有者通信手段、１５は所有者通信手段１４により入力される情報と暗号化に必要な暗号化情報１５０１を記憶する為の暗号情報記憶手段、１６０１は各端末のＩＤ番号を記憶したデータベースで端末ＩＤ番号ＤＢ、１６０２は各端末の所有者に対するパスワードを記憶したデータベースでパスワードＤＢ、１６０３はパスワードＤＢ１６０２から端末ＩＤ番号Ａ１０１で呼出されるパスワードＢ、１６は端末ＩＤ番号ＤＢ１６０１とパスワードＤＢ１６０２を記憶する端末情報記憶手段、１３０２は端末ＩＤ番号送信機能８０１から送信された端末ＩＤ番号Ｂ１２０４と所有者１が所有者通信手段１４から入力した端末ＩＤ番号Ａ１０１を照合する端末ＩＤ番号照合機能、１３０４は端末ＩＤ照合機能１３０２が照合出来た事を示す信号でＩＤ確認、１３０１はＩＤ確認１３０４を受けると暗号化情報１５０１を通信回線網６を介して携帯端末２へ送信する暗号情報送信機能、１３０３は端末ＩＤ番号Ａ１０１によって携帯端末２を呼出す端末呼出し機能、１４０１は公衆回線網４または専用端末５から所有者１が入力した端末ＩＤ番号Ａ１０１を受信し、これを端末情報記憶手段１６へ入力し、後述するパスワード確認がされると端末ＩＤ番号Ａ１０１を暗号情報記憶手段１５へ入力するＩＤ番号受信機能、１４０２はパスワードＤＢ１６０２からパスワードＢ１６０３を取出し、後述するパスワード要求１４０３を所有者１へ送信し、所有者１からパスワードＡ１０２が入力されると、パスワードＡ１０２とパスワードＢ１６０３の照合を行い確認結果をＩＤ番号受信機能１４０１へ入力するパスワード確認機能、１４０３は端末ＩＤ番号Ａ１０１の入力に対して所有者１を正規の利用者であることを認証する為のパスワードを要求する信号でパスワード要求、１４０４はパスワード確認機能１４０２がパスワードを確認出来たことを示す信号で確認である。

【００３７】次に、本実施例の動作を、図１，図２，図３を用いて説明する。

【００３８】まず本実施例で対象としているデータ通信システムでは図２に示すように、携帯端末２が情報ＤＢ１７を操作するには、最初に接続手順９０２によりホスト装置３のゲート３１と接続し、次にゲート３２で端末ＩＤ番号Ｂ１２０４を入力し、番号が確認されると携帯端末が接続され、続いて所有者パスワード９０４を入力すると情報ＤＢ１７と接続されるようになっている。

【００３９】また、ホスト装置への接続のたびに所有者パスワード９０４を入力することは、通常の利用ではかえって煩わしい場合もあるので、この場合には接続手順９０２の中に所有者パスワード９０４も含めてしまうことも可能である。

【００４０】つまり、携帯端末２は所有者１のプライベートな情報だけでなく、ホスト装置３への接続も可能な機能を備えており、第三者によって所有者パスワード９０４が破られ、利用されると損害が発生する可能性のある端末であり、接続手順に所有者パスワードが含まれるような場合は尚更である。

【００４１】以下の説明は、所有者１が携帯端末２をいずれかで紛失したことに気付いたところで、図１に示す

ようにデータ漏洩防止の操作をするところから説明する。

【００４２】そこで、所有者１は少しでも携帯端末２から情報が漏れることを防止するために、手近にある公衆回線網４またはホスト装置３の専用端末５からデータ漏洩防止の操作を行う。

【００４３】すると、この操作ではまずホスト装置３が所有者通信手段１４のＩＤ番号受信機能１４０１で、所有者１から入力された端末ＩＤ番号Ａ１０１を受信し、これを端末情報記憶手段１６へ入力する。端末ＩＤ番号Ａ１０１を入力された端末情報記憶手段１６は、端末ＩＤ番号ＤＢ１６０１とパスワードＤＢ１６０２からこの端末ＩＤ番号Ａ１０１の所有者１に登録されたパスワードＢ１６０３を取出し、これをパスワード確認機能１４０２へ入力する。

【００４４】パスワードＢ１６０３を入力されるとパスワード確認機能１４０２は、所有者１に対して公衆回線網４またはホスト装置３の専用端末５からパスワードの入力を促すパスワード要求１４０３を出力する。これに対して、所有者１がパスワードＡ１０２を入力すると、パスワード確認機能１４０２は先のパスワードＢ１６０３とパスワードＡ１０２を照合して、もし同じであることが確認できたら、すなわち、データ漏洩防止の操作をしている人物が、携帯端末２の正規の所有者であることを確認したら、これを示す信号、確認１４０４をＩＤ番号受信機能１４０１へ入力する。そして、確認１４０４を受けたＩＤ番号受信機能１４０１はこの端末が第三者に利用されることにより、データ漏洩の恐れのある端末として登録する為に、端末ＩＤ番号Ａ１０１を暗号情報記憶手段１５に記憶させる。

【００４５】この後、ホスト装置３は自ら先に記憶した端末ＩＤ番号Ａ１０１とホスト側通信手段１３の端末呼出し機能１３０３と、通信回線網６により携帯端末２を呼出すか、または不正利用者７が携帯端末２を使ってデータ記憶手段９に記憶した接続手順９０２と、通信回線網６を介してホスト装置３を呼出すかすると、携帯端末２が端末制御手段１２のＲＯＭ１２０１に予め記憶している端末ＩＤ番号Ｂ１２０４を、端末側通信手段８の端末ＩＤ番号送信機能８０１によりホスト装置３へ送信し、一方、ホスト装置３ではホスト側通信手段１３の端末ＩＤ番号照合機能１３０２が、暗号情報記憶手段１５から端末ＩＤ番号Ａ１０１を取出し、携帯端末２から送信された端末ＩＤ番号Ｂ１２０４と照合を行う。

【００４６】この照合で一致が確認されるとＩＤ確認１３０４が暗号情報送信機能１３０１へ入力され、暗号情報送信機能１３０１は暗号情報記憶手段１５に記憶されている暗号化情報１５０１を通信回線網６を介して携帯端末２へ送信する。（なお、ホスト装置３に端末ＩＤ番号が登録されていないとき、つまり通常の場合は暗号化情報１５０１に代って所有者パスワード９０４の入力が求められることになる。）携帯端末２は端末側通信手段８の受信誤りチェック機能８０２で暗号化情報１５０１を受信し、誤りの有無を確認した後、データ記憶手段９に記憶する。暗号化情報１５０１が記憶されると、端末制御手段１２はデータ記憶手段９に記憶されている、通常データ９０１と接続手順９０２を暗号化前データ９０３として取出し、これらを演算手段１２０２へ入力する。

【００４７】データを入力された演算手段１２０２は、先に記憶された暗号化情報１５０１をデータ記憶手段９から取出し、これに基づいて入力されたデータを暗号化する。

【００４８】暗号化されたデータは暗号データ１２０６となり、データ記憶手段９へ入力され、暗号化前データ９０３に上書きして記憶される。そして、すべての通常データ９０１と接続手順９０２の暗号化が終了すると、演算手段１２０２は完了１２０６を消去機能１２０３へ入力し、消去機能１２０３は消去信号１２０５を発生してデータ記憶手段９に記憶された暗号化情報１５０１を消去するので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【００４９】本実施例によれば、携帯端末を紛失後でも手近な通信手段を使ってホスト装置に紛失した事を登録すれば、後は携帯端末とホスト装置との接続が行われることにより、以後携帯端末内に記憶された所有者のプライベートな情報も、ホスト装置への接続手順も参照することが出来なくなるので、データの漏洩による損害を最小限に出来る。

【００５０】もちろん、接続をする前に不正利用者７が接続情報９０２を何らかの手段によって取出すことも有り得るが、ホスト装置と通信をするには端末ＩＤ番号Ｂ１２０４が必要である為、接続手順だけを不正利用者７が用意した第二の携帯端末に記憶させても通信は出来ず、またさらに何らかの方法で端末ＩＤ番号Ｂも取出して通信を確立したとしても、ホスト装置３からは暗号化情報１５０１が送信されるので、この第二の携帯端末のデータ記憶手段に記憶された内容も暗号化されることになる。よってこの場合、漏洩するデータは携帯端末２に記憶されていたデータに限られることになり、ホスト装置３にある情報ＤＢ１７が利用されることはない。

【００５１】なお、図示しないが所有者１が紛失したことに気が付くのが遅くなり、まだデータ漏洩防止の操作を行っていない場合でも、不正利用者７が情報ＤＢ１７への接続で、ホスト装置３から要求される所有者パスワード９０４の入力を、予めホスト装置３で決められている回数を越えて失敗したかどうかを判断するようにすることで、たとえ所有者１からの操作が無くても上記の暗号化処理を自動的に行うようにしてもよい。

【００５２】さらに、すでに所有者１によりデータ漏洩防止の操作がなされているときに、不正利用者７がホス

ト装置３への接続を試みると、上記のごとく携帯端末２では暗号化処理が行われるが、このときデータ表示手段１０には既にホスト装置３との接続は完了していても、例えば「ただ今ホスト装置への接続処理中です」と言ったメッセージを表示し続け、暗号化処理中であることを悟られないようにすることで、犯罪を目的として操作したのではない不正利用者７に不要な不愉快感を与えさせないようにもできる。

【００５３】また、暗号化情報１５０１を暗号化プログラムと暗号化時の係数となる暗号キーとすれば、図４に示すように暗号情報記憶手段１５に暗号化プログラム１５０２と暗号キー１５０３を予め記憶しておき、これらを暗号化情報１５０１として送信し、携帯端末２ではデータ記憶手段９がこれらを記憶して、演算手段１２０２が暗号化プログラム１５０２を実行し、暗号キー１５０３を係数として暗号化前データ９０３を暗号データ１２０６に変換するようにすれば、暗号化のためのプログラムを内蔵していない携帯端末でもデータの漏洩を防止できることになる。

【００５４】また、これに端末ＩＤ番号による機種判別を加えれば、機種毎の暗号化プログラムをホスト装置が用意することも可能である。

【００５５】さらに、図示しないが暗号化プログラムを内蔵している場合には、暗号化情報１５０１として暗号キー１５０３と暗号化プログラムに起動を掛けるための制御コマンドを用いることも可能で、この場合には携帯端末２が暗号キー１５０３と制御コマンドといった簡単なデータを受信するだけで済むので接続時間が短くなり、それだけ通信費が安くなる。

【００５６】またさらに、上記とは逆に暗号キーを既に内蔵している場合には、暗号化情報１５０１として暗号化プログラム１５０２を用いることも可能で、この場合には多少接続時間は長くなるが、同じ暗号キーでも暗号化のアルゴリズムを自由に変更できるので、常に最新方式の暗号化を所有者１に提供できるとともに、万が一プログラムにバグがある場合にも対応が簡単にできるようになる。

【００５７】＜第２実施例＞図５は、本発明の第二実施例のデータ漏洩防止システムにおける、データの復号化動作の説明図である。

【００５８】図５で、１５０４は携帯端末２が暗号データ１２０６を復号化するために使う復号化情報、１２０７は演算手段１２０２が暗号データ１２０６を復号化した復号化後データである。また、第一実施例と異なり、ＩＤ番号受信機能１４０１にはホスト側通信手段１３へ端末ＩＤ番号Ａ１０１を出力する機能、暗号情報送信機能１３０１にはＩＤ確認１３０４を受けると復号化情報１５０４を通信回線網６を介して携帯端末２へ送信する機能を有する。

【００５９】次に本実施例の動作を図５を用いて説明する。なお本実施例では、携帯端末２のデータ記憶手段９には既に暗号化されたデータ、つまり暗号データ１２０６として記憶されており、所有者１がこれを復号化したいと思っている場合とする。

【００６０】まず、所有者１は第一実施例と同様に手近な公衆回線網４または専用端末５からホスト装置３を呼び出し、端末ＩＤ番号Ａ１０１を入力する。すると、ホスト装置３からパスワード要求１４０３があり、これに対してパスワードＡ１０２を入力すると、所有者通信手段１４で照合がなされ、確認されると端末ＩＤ番号Ａ１０１はホスト側通信手段１３の端末呼出機能１３０３へ入力される。

【００６１】そして端末呼出機能１３０３が通信回線網６を介して、端末ＩＤ番号Ａ１０１で携帯端末２を呼び出すと、端末からこれに対する応答として端末ＩＤ番号Ｂ１２０４が端末ＩＤ送信機能８０１と通信回線網６を介して返送されるので、これを受信したホスト側通信手段１３は端末ＩＤ番号照合機能１３０２で、端末ＩＤ番号Ａ１０１と端末ＩＤ番号Ｂ１２０４の照合を行い、正しく照合がされるとＩＤ確認１３０４が暗号情報送信機能１３０１に入力される。

【００６２】すると、ＩＤ確認１３０４を受けた暗号情報送信機能１３０１は、暗号情報記憶手段１５に予め記憶していた復号化情報１５０４を通信回線網６を介して携帯端末２へ送信するので、携帯端末２はこれを端末側通信手段８で受信し、受信誤りチェック機能８０２で確認した後、データ記憶手段９に記憶する。

【００６３】復号化情報１５０４が記憶されると、端末制御手段１２の演算手段１２０２がデータ記憶手段９から暗号データ１２０６と復号化情報１５０４を取り出し、復号化処理を実行して復号化後データ１２０７に変換し、暗号化データ１２０６に上書きして記憶する。

【００６４】以上の様に本実施例によれば、携帯端末２をデータ漏洩から守る為に行った暗号化処理を手近な通信手段から簡単にいつでも解除することが可能になる。

【００６５】また、復号化の情報が第三者には簡単に操作できないホスト装置に記憶されているので、所有者に情報を覚える煩わしさを持たせずに安全にデータを守ることが出来る。

【００６６】なお図示はしないが、ここで復号化情報１５０４は第一実施例の図４の場合に対応して、復号化プログラムと暗号化に使った暗号キーとすることも、また端末が暗号キーを内蔵しているときには復号化プログラムだけとすることも可能で、さらに端末ＩＤ番号により携帯端末の種類を特定できれば、機種毎に対応したプログラムを送信することも第一実施例と同様に可能になることは容易に想像できることである。

【００６７】＜第３実施例＞図６は、本発明の第三実施例のデータ漏洩防止システムにおける、データの暗号化動作の説明図である。

【００６８】図６で、１５０５は携帯端末２のデータ記憶手段９にある暗号化情報１５０１を端末制御手段１２に消去するように命令する為の消去コマンド、１３０５はＩＤ確認１３０４を受けて消去コマンド１５０５を携帯端末２へ送信する消去コマンド送信機能である。

【００６９】また、第一実施例と異なり、端末制御手段１２の消去機能１２０３は消去コマンド１５０５を受けると起動する機能、演算手段１２０２は暗号化情報１５０１にある情報により暗号化と復号化の両方を実行する機能を有する。

【００７０】本実施例が第一実施例と異なる点は、携帯端末が暗号化と復号化の機能を予め内蔵しており、入力手段から入力されるか、内部の演算によって得られたデータを必ず暗号化してから記憶手段に記憶させ、記憶されたデータを所有者に提示するなど必要なときだけ復号化する機能を有し、万が一の場合には暗号化と復号化の処理で使用する暗号化情報を消去することが可能な点にある。

【００７１】次に、本実施例の動作を図６を用いて説明する。なお、本実施例も第一実施例と同様に、所有者１が携帯端末２をいずれかで紛失したことに気付いたところであるとする。

【００７２】そこで、所有者１が第一実施例と同様に手近にある公衆回線網４またはホスト装置３の専用端末５からデータ漏洩防止の操作を行うと、端末ＩＤ番号Ａ１０１の入力に続いてパスワード要求１４０３を受け、パスワードＡ１２０を入力すると端末ＩＤ番号Ａ１０１が暗号情報記憶手段１５に記憶される。

【００７３】この後も第一実施例と同様に、ホスト装置３から携帯端末２を呼出すか、または不正利用者７が接続手順９０２によりホスト装置３を呼出すかすると、端末ＩＤ番号照合機能１３０２により端末ＩＤ番号の照合がなされ、一致が確認されると、暗号情報記憶手段１５に記憶されている消去コマンド１５０５が取出され、消去コマンド送信機能１３０５がこのコマンドを通信回線網６を介して携帯端末２へ送信する。

【００７４】一方、消去コマンド１５０５を受信した端末側通信手段８は、同コマンドを端末制御手段１２の消去機能１２０３へ入力する。そして、消去機能１２０３が起動して消去信号１２０５をデータ記憶手段９へ入力すると、暗号情報１５０１が消去されるので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【００７５】本実施例によれば、携帯端末内のデータは既に暗号化されているので、暗号化処理のための時間が不要であり、紛失後でも手近な通信手段を使ってホスト装置に紛失した事を登録すれば、後は携帯端末とホスト装置との接続が行われることにより、携帯端末内に記憶された所有者のプライベートな情報も、ホスト装置への接続手順も瞬時に参照することが出来なくなるので、データの漏洩による損害を最小限に出来る。

【００７６】また本実施例の場合ホスト装置から送信するデータは暗号情報を消去させるコマンドだけなので、全く機種の異なる携帯端末でも同コマンドの仕様だけ規定されていれば、ホスト装置側で機種別対応をしなくても、上記のようにデータの漏洩防止を図ることが可能になる。

【００７７】＜第４実施例＞図７は、本発明の第四実施例のデータ漏洩防止システムにおける、データの暗号化動作の説明図である。

【００７８】図７で、１１０２は所有者１がデータ入力手段１１から入力した暗号化情報、１１０１は所有者１が携帯端末２に対して内蔵するデータを暗号化するように命令する暗号化要求、１２０８は暗号化情報１１０２の入力を所有者１に要求する暗号情報入力要求、１２０９は端末側通信手段８にホスト装置３の呼出しと暗号化情報１１０２の送信を命令する暗号化開始指示、８０３はデータ記憶手段９に記憶された暗号化情報１１０２をホスト装置３へ送信する復号化情報送信機能、８０４は暗号化情報１１０２の送信が完了したことを演算手段１２０２へ通知するための送信終了、１５０４は暗号化情報１１０２と同じ情報で復号化のためにホスト装置３に記憶された復号化情報、１３０６は復号化情報１５０４を通信回線網６を介して受信して、ＩＤ確認１３０４が端末ＩＤ番号照合機能１３０２から出力されると、暗号情報記憶手段１５に端末ＩＤ番号Ｂ１２０４と関連付けて記憶させる復号化情報受信機能である。また、端末制御手段１２に暗号化要求１１０１を受けると暗号情報入力要求１２０８をデータ表示手段１０を介して所有者１に提示する機能と、暗号化情報１１０２の入力を受けると暗号化開始指示１２０９を出力する機能を有する。

【００７９】本実施例が第一実施例と異なる点は、所有者が携帯端末を紛失した後にデータ漏洩防止の操作をするのではなく、紛失や盗難の可能性に対して予めデータ漏洩の防止をする点にある。

【００８０】次に、本実施例の動作を図７を用いて説明する。ここでは、例えば所有者１が空港で手荷物を預ける際に、万が一の場合を考慮して手元にある携帯端末２内のデータを暗号化させようとしているとする。

【００８１】まず、所有者１はデータ入力手段１１から暗号化要求１１０１を入力する。すると、端末制御手段１２から暗号情報入力要求１２０８がデータ表示手段１０を介して所有者１に提示される。所有者１がこの要求に対して暗号化情報１１０２をデータ入力手段１１から入力すると、端末制御手段１２から端末側通信手段８に暗号化開始指示１２０９が入力される。指示を受けた通信手段は、接続手順９０２によって通信回線網６を介してホスト装置３と接続を行い、端末ＩＤ番号送信機能８０１により端末ＩＤ番号Ｂ１２０４の送信を行い、また復号化情報送信機能８０３によって暗号化情報１１０２

を復号化情報１５０４としてホスト装置３へ送信する。

【００８２】一方、端末ＩＤ番号Ｂ１２０４を受信したホスト装置３では、端末ＩＤ番号照合機能１３０２で端末ＩＤ番号Ｂ１２０４が端末ＩＤ番号ＤＢ１６０１に登録されているか否かを確認し、登録されている場合にはＩＤ確認１３０４を復号化情報受信機能１３０６に入力し、端末ＩＤ番号Ｂ１２０４を暗号化情報記憶手段１５に記憶させる。そして復号化情報受信機能１３０６は受信した復号化情報１５０４を先の端末ＩＤ番号Ｂ１２０４と対応させて記憶する。

【００８３】また、復号化情報１５０４の送信を完了した携帯端末２では、端末側通信手段８が演算手段１２０２に暗号化処理を開始させる為に送信終了８０４を入力し、演算手段１２０２は第一実施例と同様に暗号化情報１１０２により暗号化前データ９０３を暗号データ１２０６へ変換し、データ記憶手段９へ入力して暗号化前データ９０３に上書き記憶する。そして、すべての通常データ９０１と接続手順９０２の暗号化が終了すると、演算手段１２０２は完了１２０６を消去機能１２０３へ入力し、消去機能１２０３は消去信号１２０５を発生してデータ記憶手段９に記憶された暗号化情報１５０１を消去するので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【００８４】本実施例によれば、携帯端末内のデータを損害が生じる前に、しかも所有者が望むときに予め暗号化することが出来るので、手荷物が盗難に遭うような事があってもデータが漏洩する恐れがなくなり、安心して預けることが出来る。

【００８５】また、本実施例と第二実施例を組合せれば、本実施例で示すように暗号化した後、任意の時点で所有者が第二実施例のように復号化をホスト装置に依頼することでデータを回復できるといった使い勝手を実現でき、この場合復号化に使用する情報は暗号化されている間、ホスト装置に保持されるので第三者がこれを取出すことは困難であり、データ漏洩に対する安全性が高いシステムを提供できる。

【００８６】なお、データ記憶手段９は、フラッシュＲＯＭやＥＥＰＲＯＭといった半導体デバイス、またはハードディスクや光磁気ディスクと言ったストレージデバイスであってもよい。

【００８７】また、通信回線網６を介して端末とホスト装置を接続する手段にはセルラー無線、パーソナル・ハンディフォン・システム（ＰＨＳ）、無線ＬＡＮ、有線ＬＡＮなど考えられる。

【００８８】

【発明の効果】本発明によれば、携帯端末の所有者は端末の紛失や盗難に伴うデータ漏洩を最小限にとどめることが可能になる。また、そのための操作も手近な通信手段を用いてホスト装置に依頼するだけであり、所有者に負担を感じさせない安心感を提供できる。

【図面の簡単な説明】

【図１】本発明の概略の説明図。

【図２】本発明の携帯端末とホスト装置の接続の説明図。

【図３】本発明の第一実施例の説明図。

【図４】本発明の第一実施例の補足説明図。

【図５】本発明の第二実施例の説明図。

【図６】本発明の第三実施例の説明図。

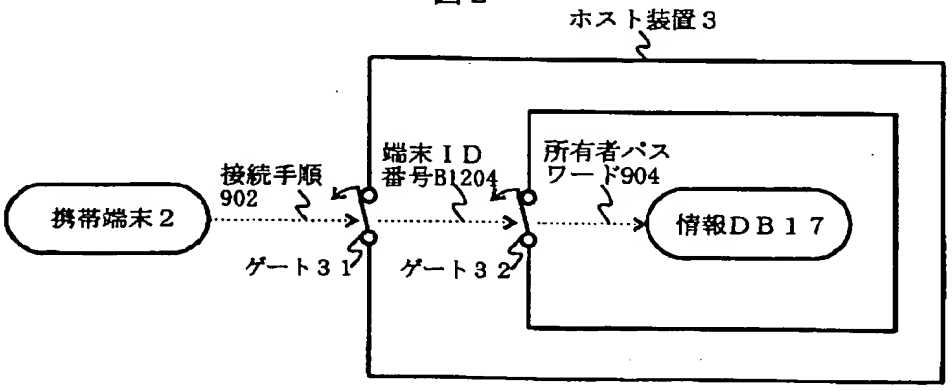
【図７】本発明の第四実施例の説明図。

【符号の説明】

１…所有者、２…携帯端末、３…ホスト装置、４…公衆回線網、５…専用端末、６…通信回線、７…不正利用者、８…端末側通信手段、９…データ記憶手段、１２…端末制御手段、１３…ホスト側通信手段、１４…所有者通信手段、１５…暗号情報記憶手段、１６…端末情報記憶手段。

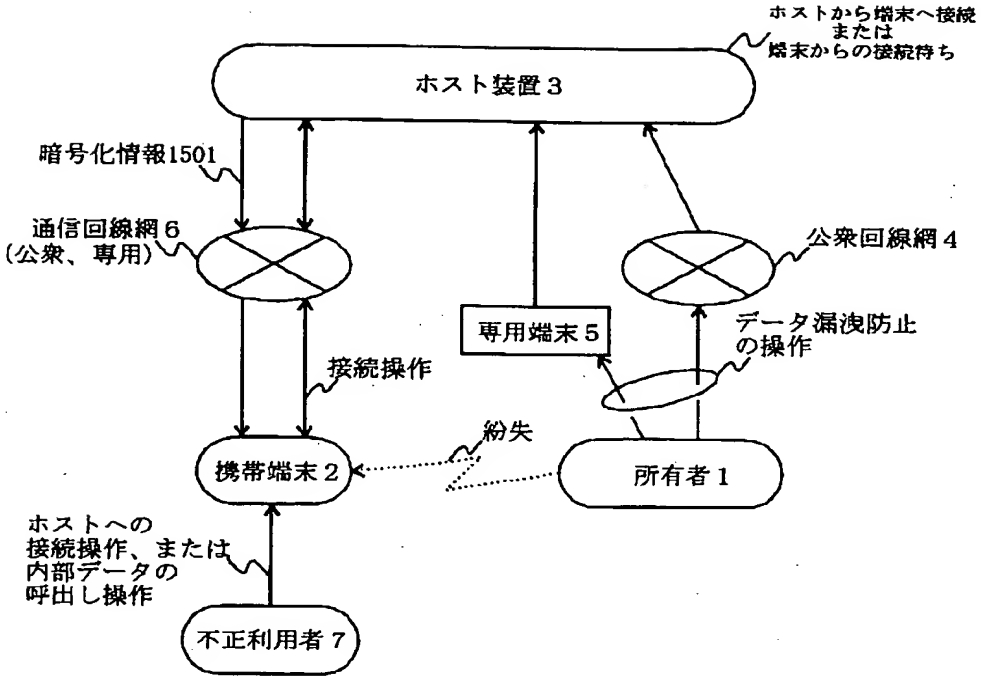
【図２】

図２



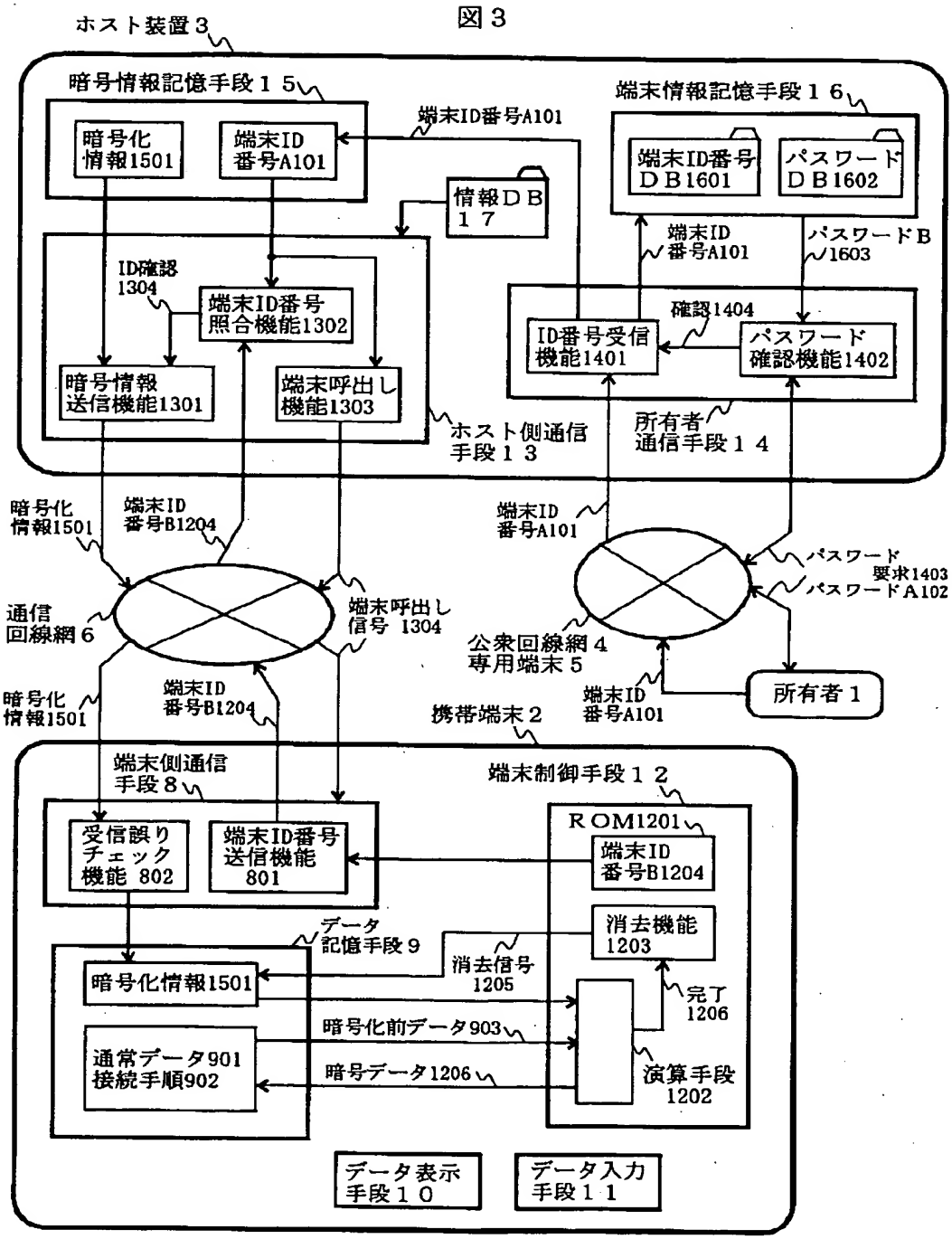
【図１】

図１


ホストから端末へ接続
または
端末からの接続待ち
ホスト装置３
暗号化情報1501
通信回線網６
（公衆、専用）
公衆回線網４
専用端末５
データ漏洩防止
の操作
接続操作
紛失
携帯端末２
所有者１
ホストへの
接続操作、または
内部データの
呼出し操作
不正利用者７

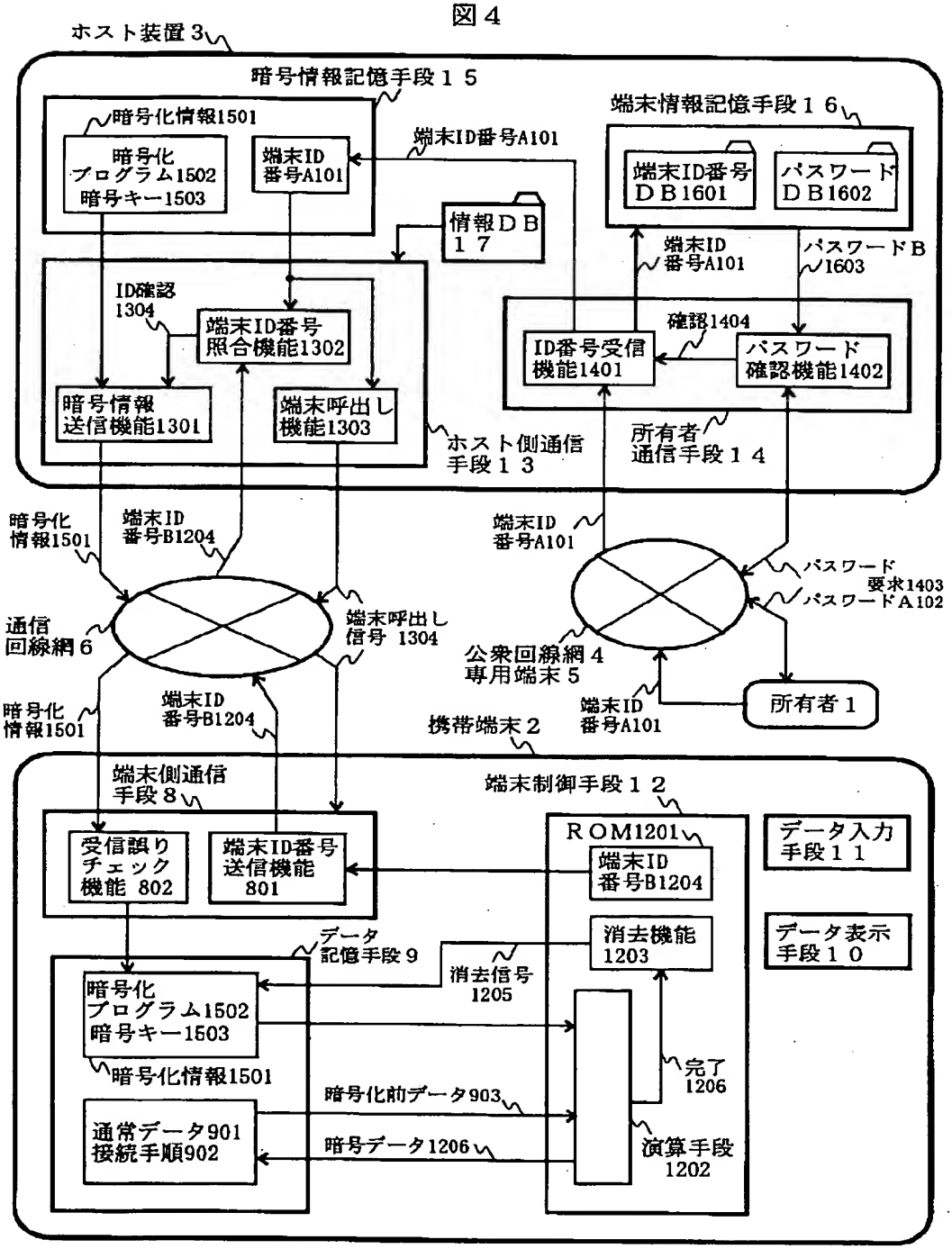
【図３】

図３


ホスト装置３
暗号情報記憶手段１５
暗号化情報1501
端末ID番号A101
端末ID番号A101
情報ＤＢ１７
端末情報記憶手段１６
端末ID番号ＤＢ1601
パスワードＤＢ1602
端末ID番号A101
パスワードB1603
ID確認1304
端末ID番号照合機能1302
確認1404
ID番号受信機能1401
パスワード確認機能1402
暗号情報送信機能1301
端末呼出し機能1303
ホスト側通信手段１３
所有者通信手段１４
暗号化情報1501
端末ID番号B1204
端末ID番号A101
パスワード要求1403
パスワードA102
通信回線網６
端末呼出し信号 1304
公衆回線網４
専用端末５
所有者１
暗号化情報1501
端末ID番号B1204
端末ID番号A101
携帯端末２
端末側通信手段８
端末制御手段１２
受信誤りチェック機能 802
端末ID番号送信機能 801
ROM1201
端末ID番号B1204
データ記憶手段９
消去機能1203
消去信号1205
暗号化情報1501
完了1206
暗号化前データ903
通常データ901
接続手順902
暗号データ1206
演算手段1202
データ表示手段１０
データ入力手段１１

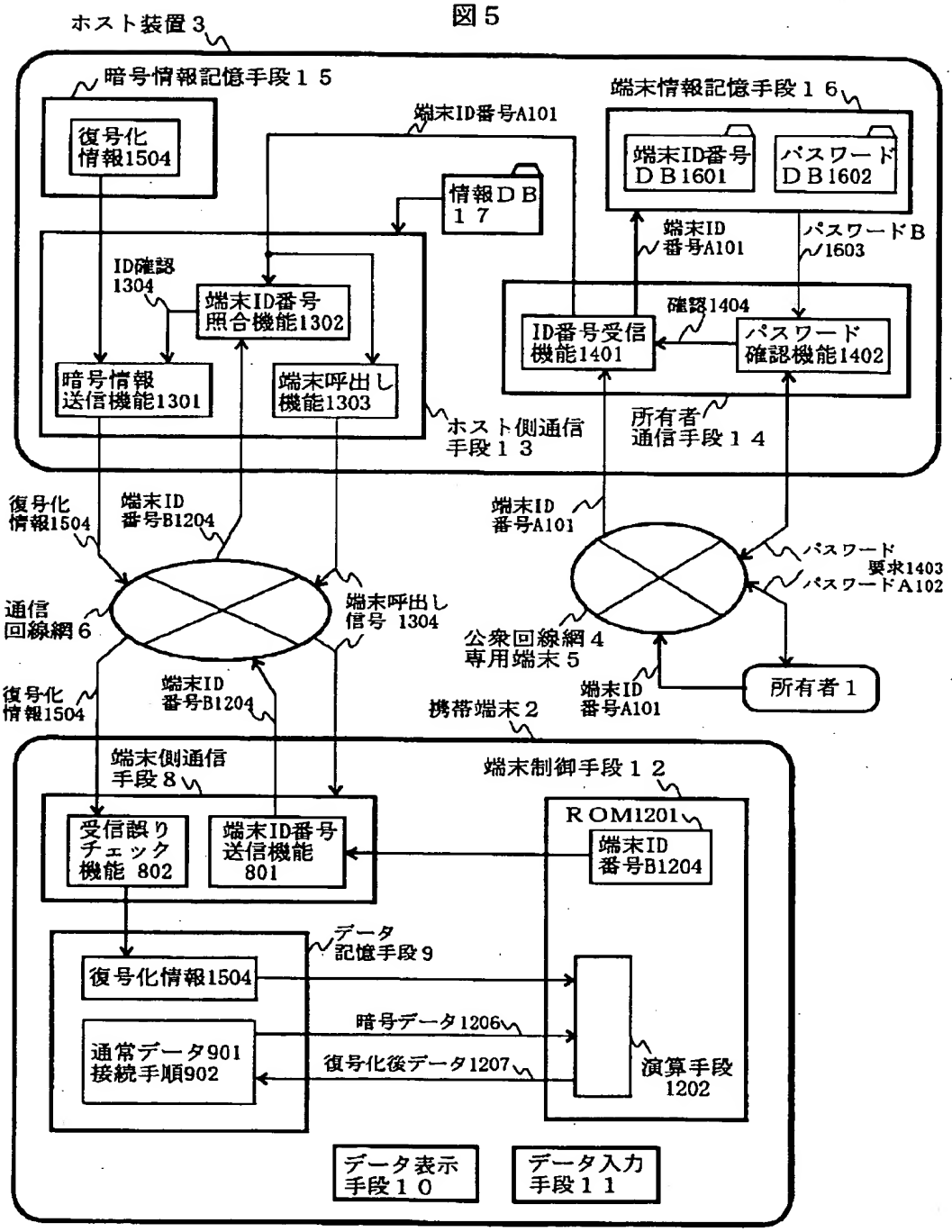
【図４】

図４


ホスト装置３
暗号情報記憶手段１５
暗号化情報1501
暗号化
プログラム1502
暗号キー1503
端末ID
番号A101
端末ID番号A101
情報ＤＢ
１７
端末情報記憶手段１６
端末ID番号
ＤＢ1601
パスワード
ＤＢ1602
端末ID
番号A101
パスワードB
1603
ID確認
1304
端末ID番号
照合機能1302
確認1404
ID番号受信
機能1401
パスワード
確認機能1402
暗号情報
送信機能1301
端末呼出し
機能1303
ホスト側通信
手段１３
所有者
通信手段１４
暗号化
情報1501
端末ID
番号B1204
端末ID
番号A101
パスワード
要求1403
パスワードA102
通信
回線網６
端末呼出し
信号 1304
公衆回線網４
専用端末５
暗号化
情報1501
端末ID
番号B1204
端末ID
番号A101
所有者１
携帯端末２
端末側通信
手段８
端末制御手段１２
受信誤り
チェック
機能 802
端末ID番号
送信機能
801
ＲＯＭ1201
端末ID
番号B1204
データ入力
手段１１
消去機能
1203
データ表示
手段１０
データ
記憶手段９
消去信号
1205
暗号化
プログラム1502
暗号キー1503
暗号化情報1501
完了
1206
暗号化前データ903
通常データ901
接続手順902
暗号データ1206
演算手段
1202

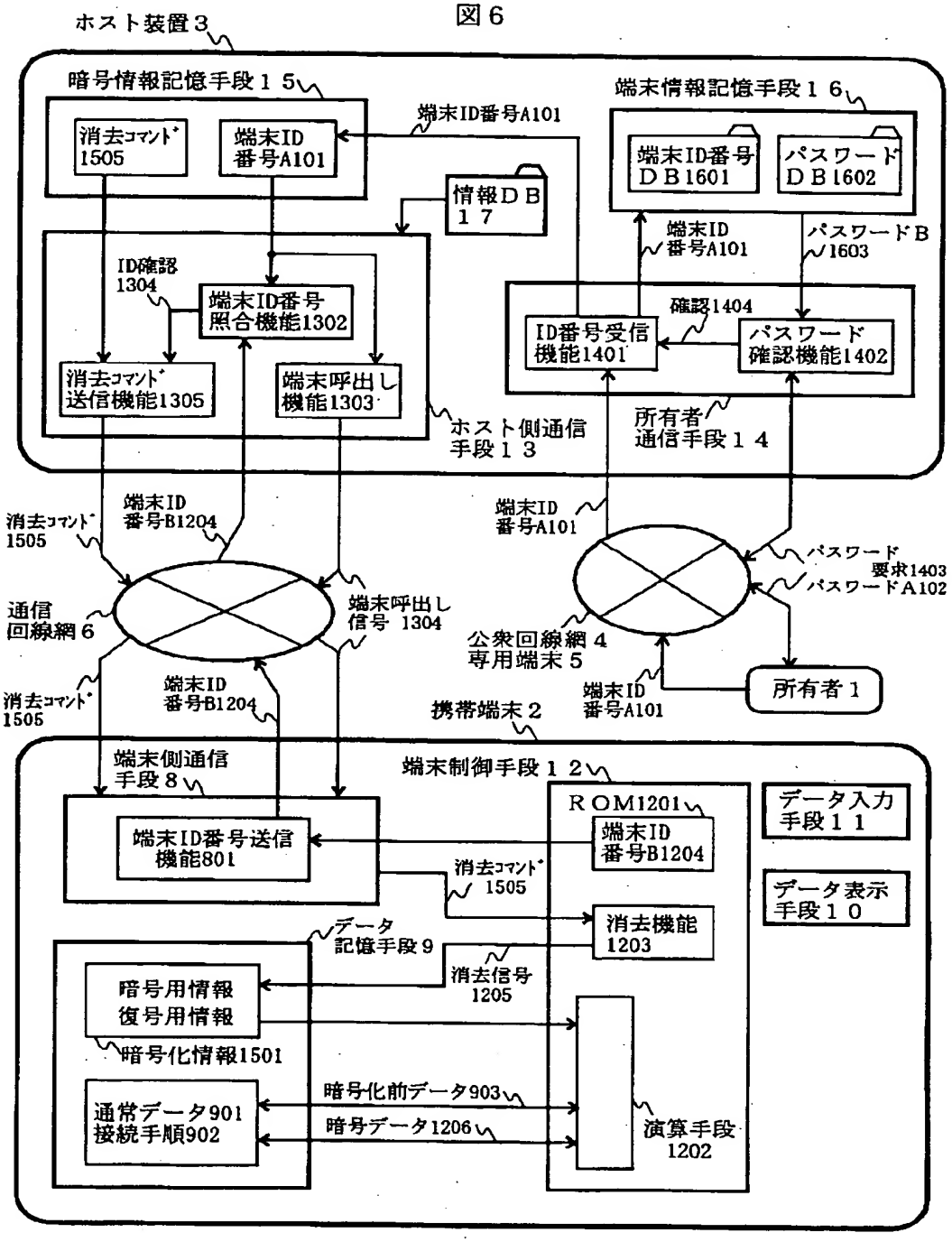
【図５】

図５


ホスト装置３
暗号情報記憶手段１５
復号化情報1504
端末ID番号A101
情報ＤＢ１７
端末情報記憶手段１６
端末ID番号ＤＢ1601
パスワードＤＢ1602
端末ID番号A101
パスワードB1603
ID確認1304
端末ID番号照合機能1302
確認1404
ID番号受信機能1401
パスワード確認機能1402
暗号情報送信機能1301
端末呼出し機能1303
ホスト側通信手段１３
所有者通信手段１４
復号化情報1504
端末ID番号B1204
端末ID番号A101
パスワード要求1403
パスワードA102
通信回線網６
端末呼出し信号 1304
公衆回線網４
専用端末５
所有者１
復号化情報1504
端末ID番号B1204
端末ID番号A101
携帯端末２
端末側通信手段８
端末制御手段１２
受信誤りチェック機能 802
端末ID番号送信機能 801
ROM1201
端末ID番号B1204
データ記憶手段９
復号化情報1504
暗号データ1206
通常データ901
接続手順902
復号化後データ1207
演算手段1202
データ表示手段１０
データ入力手段１１

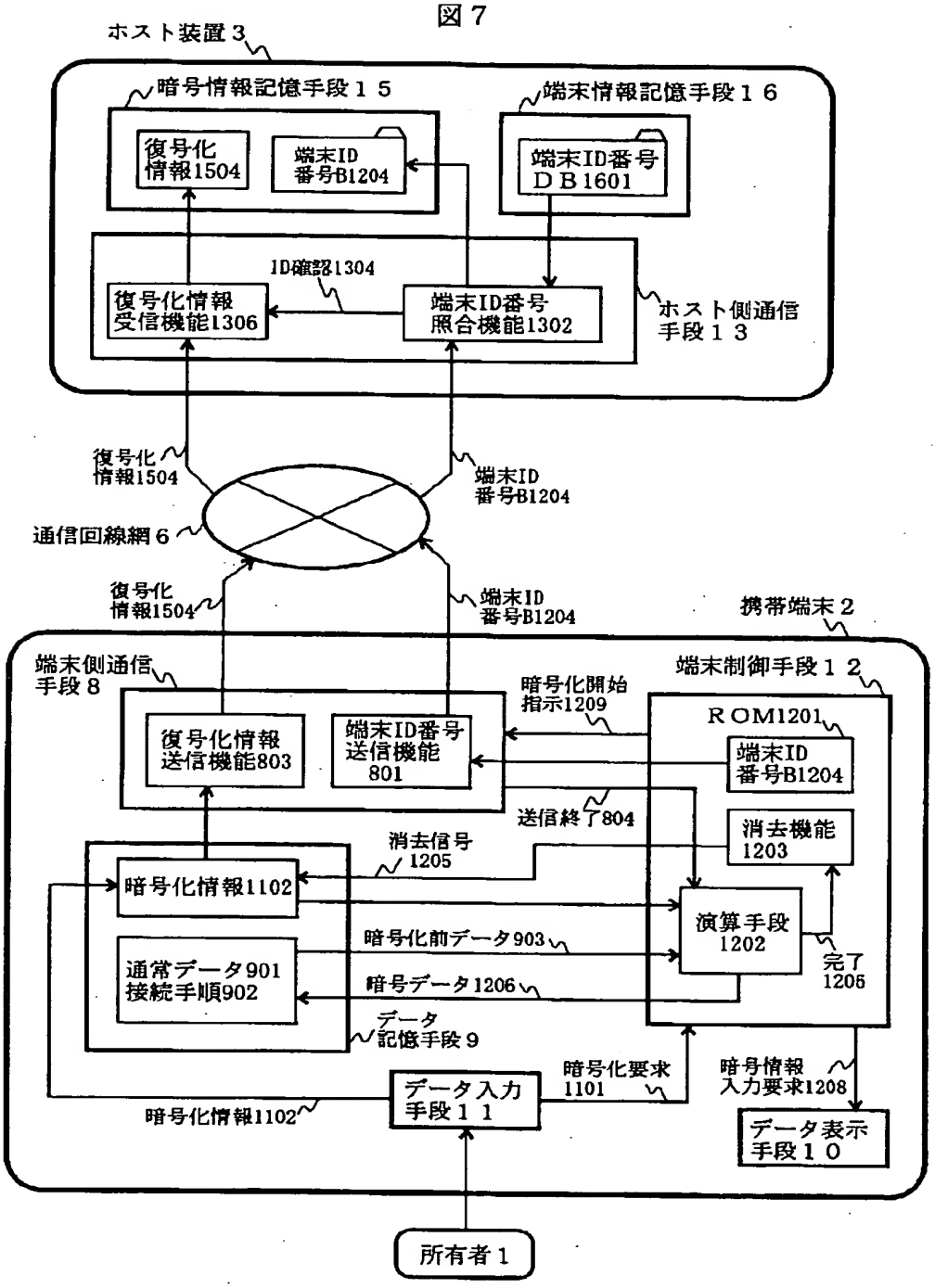
【図６】

図６


ホスト装置３
暗号情報記憶手段１５
消去ｺﾏﾝﾄﾞ 1505
端末ID 番号A101
端末ID番号A101
情報ＤＢ １７
端末情報記憶手段１６
端末ID番号 ＤＢ1601
パスワード ＤＢ1602
端末ID 番号A101
パスワードB 1603
ID確認 1304
端末ID番号 照合機能1302
確認1404
ID番号受信 機能1401
パスワード 確認機能1402
消去ｺﾏﾝﾄﾞ 送信機能1305
端末呼出し 機能1303
ホスト側通信 手段１３
所有者 通信手段１４
消去ｺﾏﾝﾄﾞ 1505
端末ID 番号B1204
端末ID 番号A101
パスワード 要求1403
パスワードA102
通信 回線網６
端末呼出し 信号 1304
公衆回線網４ 専用端末５
所有者１
消去ｺﾏﾝﾄﾞ 1505
端末ID 番号B1204
端末ID 番号A101
携帯端末２
端末側通信 手段８
端末制御手段１２
ROM1201
データ入力 手段１１
端末ID番号送信 機能801
端末ID 番号B1204
消去ｺﾏﾝﾄﾞ 1505
データ 記憶手段９
消去機能 1203
データ表示 手段１０
消去信号 1205
暗号用情報 復号用情報
暗号化情報1501
暗号化前データ903
通常データ901 接続手順902
暗号データ1206
演算手段 1202

【図７】

図７


ホスト装置３
暗号情報記憶手段１５
端末情報記憶手段１６
復号化情報1504
端末ID番号B1204
端末ID番号DB1601
ID確認1304
復号化情報受信機能1306
端末ID番号照合機能1302
ホスト側通信手段１３
復号化情報1504
端末ID番号B1204
通信回線網６
復号化情報1504
端末ID番号B1204
携帯端末２
端末側通信手段８
端末制御手段１２
暗号化開始指示1209
ROM1201
端末ID番号B1204
復号化情報送信機能803
端末ID番号送信機能801
送信終了804
消去機能1203
消去信号1205
暗号化情報1102
演算手段1202
暗号化前データ903
通常データ901
接続手順902
暗号データ1206
完了1205
データ記憶手段９
暗号化要求1101
暗号情報入力要求1208
データ入力手段１１
暗号化情報1102
データ表示手段１０
所有者１